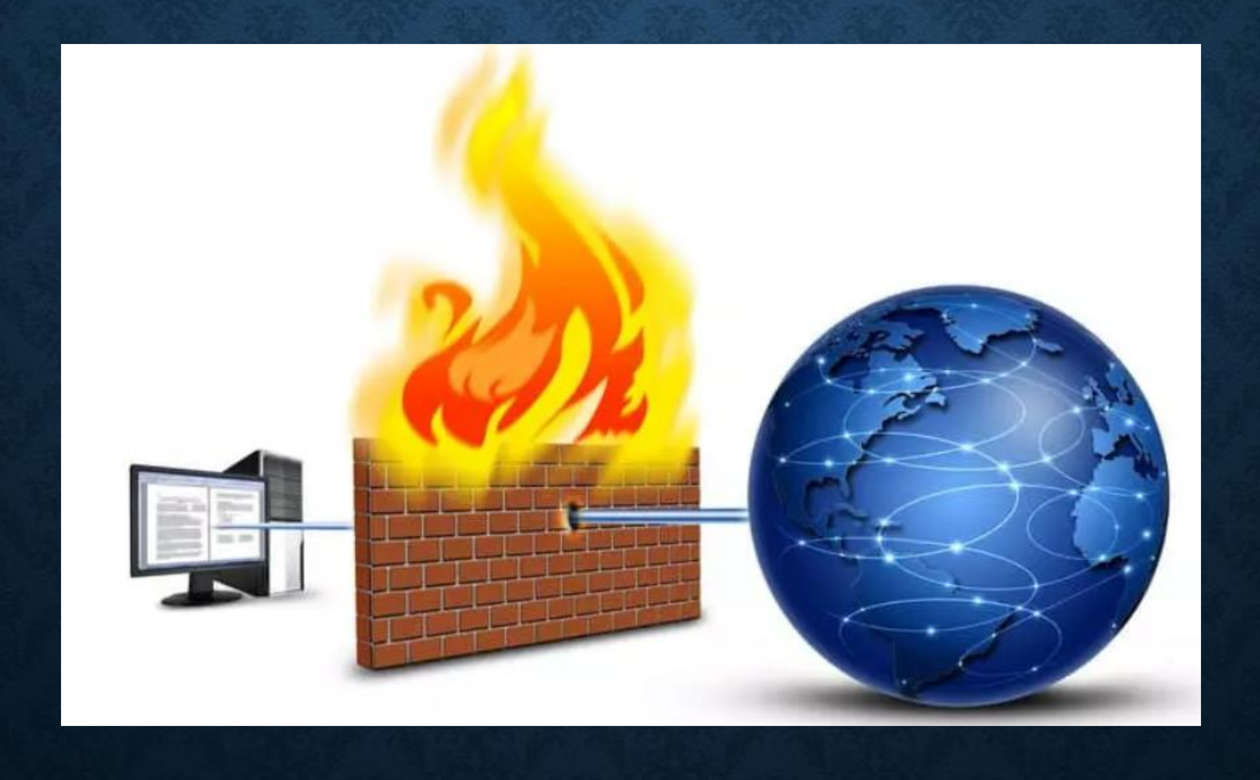
PARE-FEU (FIREWALL)



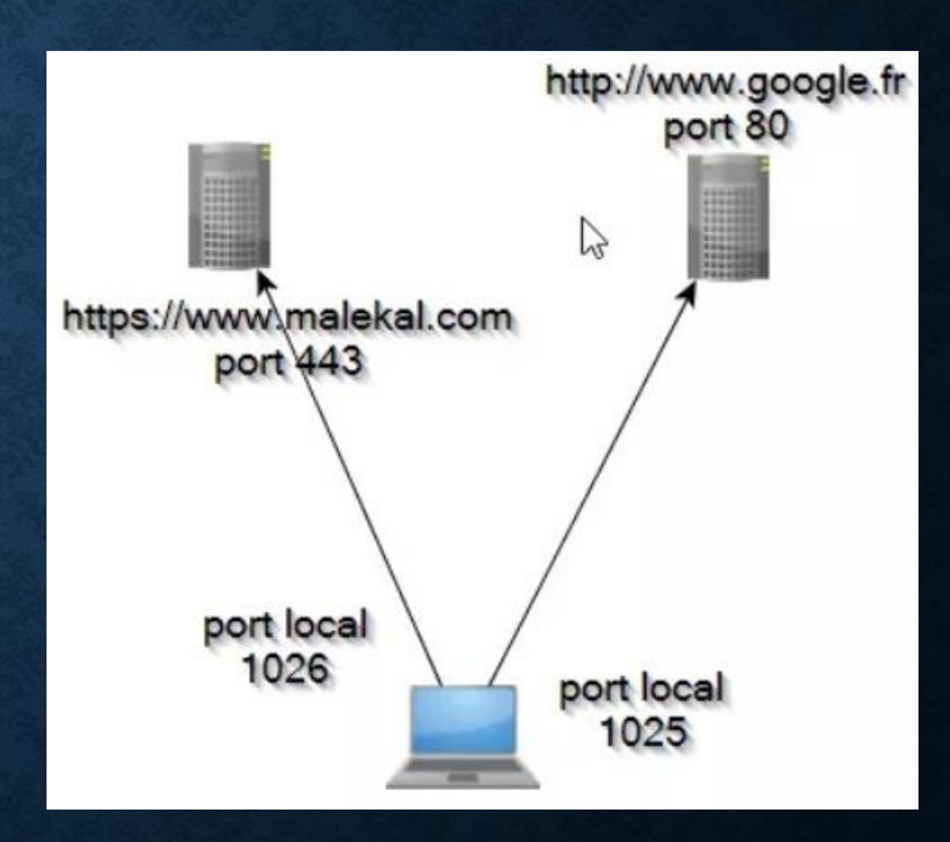
1- LES PORTS RÉSEAUX

- Lorsque l'on intéresse à la sécurité informatique, on peut entendre parler de **port réseau ouvert.**
- En effet, cela peut être utilisé comme porte d'entrée afin de s'introduire dans votre système et de pirater votre ordinateur.



LES PORTS RÉSEAUX

- Un port réseau est **un point d'entré ou de sortie réseau** qu'une application ou le système d'exploitation peut utiliser.
- Ce dernier se caractérise par un numéro, par exemple, un serveur WEB tourne sur le port 80 (HTTP) ou 443 (HTTP), un serveur FTP le port 21.
- Lorsque vous établissez une connexion vers une machine distance, vous vous connectez à un port distant en particulier.



LES PORTS RÉSEAUX – LISTE DES PORTS

- Il existe **65535** numéro de ports.
- Vous pouvez les consulter en utilisant ce line:

https://www.crashdebug.fr/liste-des-ports-logiciels-tcp-et-udp

PORT	SERVICE	DESCRIPTION
20	FTP Data	Port used by the FTP protocol to send data to a client
22	SSH	Used as secure replacment protocol for Telnet
23	Telnet	Port used by Telnet to remotely connect to a workstation or server
25	SMTP	Port used to **send** e-mail over the internet
53	DNS	Port used for DNS requests and zone transfers
80	HTTP	Protocol used for showing web pages on a browser
110	POP3	Post Office Protocol (POP3) is used to **receive/read** e-mail
143	IMAP	Internet Message Access Protocol (IMAP) is a new protocol to read e-mail
443	HTTPS	Port used for securing web traffic
3389	RDP	Port used by Remote Desktop to remotely manage a windows system

LES PORTS RÉSEAUX - ÉTATS DES PORTS

- Un **port ouvert** est donc un port **en écoute** et attente de connexion entrante.
- Par défaut Windows ou Mac ouvre des ports liés à des services réseaux. (Example: Chrome, Teams, Skype, …) . Il est donc normal d'avoir des ports ouverts.
- Les ports réseaux ont plusieurs états:
  - **Port Ouvert :** Une application a ouvert le port et ce dernier est en écoute. Un client peut alors se connecter à ce port. Comme les serveurs Web qui écoute sur le port ouvert 80.
  - **Port Fermé:** Le port est fermé et n'accepte aucune connexion entrante.
  - **Port Filtré:** Une application réseau, comme un pare-feu (firewall), filtre l'accès sur le port. Ainsi, vous n'êtes pas capable de déterminer si le port est ouvert ou fermé.

LES PORTS RÉSEAUX - ÉTATS DES PORTS

Voici la procédure pour lister les ports ouvert sur Windows:

- Ouvrez le **Gestionnaire de tâches** puis onglet **Performances.**
- Cliquez en bas à gauche sur **Moniteur de ressources.**
- Ensuite cliquez sur l'onglet **Réseau.**
- En bas, vous avez **Connexion TCP.** Vous obtenez la liste des ports ouvert et en écoute.

Connexions TCP

Processus	PID	Adresse locale	Port local	Adresse distante	Port distant
chrome.exe	3000	192.168.2.101	55531	172.217.13.162	443
chrome.exe	3000	192.168.2.101	55167	172.217.13.164	443
chrome.exe	3000	192.168.2.101	55152	172.217.13.110	443
chrome.exe	3000	192.168.2.101	55035	172.217.13.162	443
chrome.exe	3000	192.168.2.101	54149	104.17.8.65	443
chrome.exe	3000	192.168.2.101	53996	104.17.7.65	443
vpnagent.exe	4432	Bouclage IPv4	62522	Bouclage IPv4	49780
svchost.exe (netsvcs -p)	5884	192.168.2.101	53649	52.177.165.30	443
OpenVPNConnect.exe	7536	Bouclage IPv4	60790	Bouclage IPv4	60789
OpenVPNConnect.exe	7536	Bouclage IPv4	60789	Bouclage IPv4	60790
svchost.exe (UnistackSvcGroup)	8744	192.168.2.101	55517	52.179.236.206	443
svchost.exe (UnistackSvcGroup)	8744	192.168.2.101	55037	52.179.236.206	443
OUTLOOK.EXE	9344	192.168.2.101	58560	52.96.88.162	443
OUTLOOK.EXE	9344	192.168.2.101	51061	40.100.162.178	443
OUTLOOK.EXE	9344	192.168.2.101	50755	52.96.88.130	443
CcmExec.exe	11504	192.168.2.101	58550	192.168.99.111	80
Teams.exe	13788	192.168.2.101	58476	52.113.206.43	443
Teams.exe	13788	192.168.2.101	64640	52.114.128.81	443
Teams.exe	13788	192.168.2.101	63425	52.113.194.132	443
OneDrive.exe	14456	192.168.2.101	53892	52.177.166.224	443

LES PORTS RÉSEAUX - SCAN DES PORTS

- Puisque le service est en court de fonctionnement et en attente de connexion, ce dernier peut permettre une intrusion.

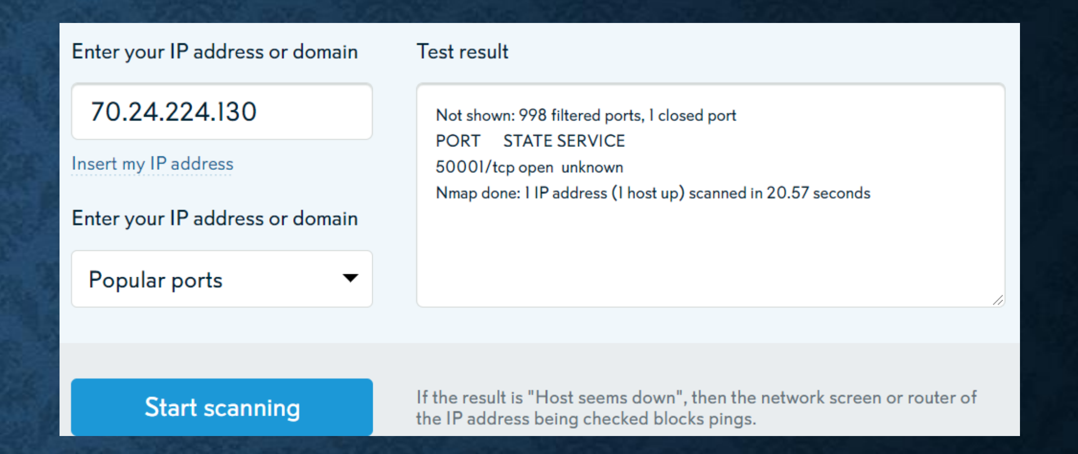
- Si le service compte une vulnérabilité, un pirate peut exploiter celle-ci pour exécuter un logiciel malveillant ou s'introduire dans le système.

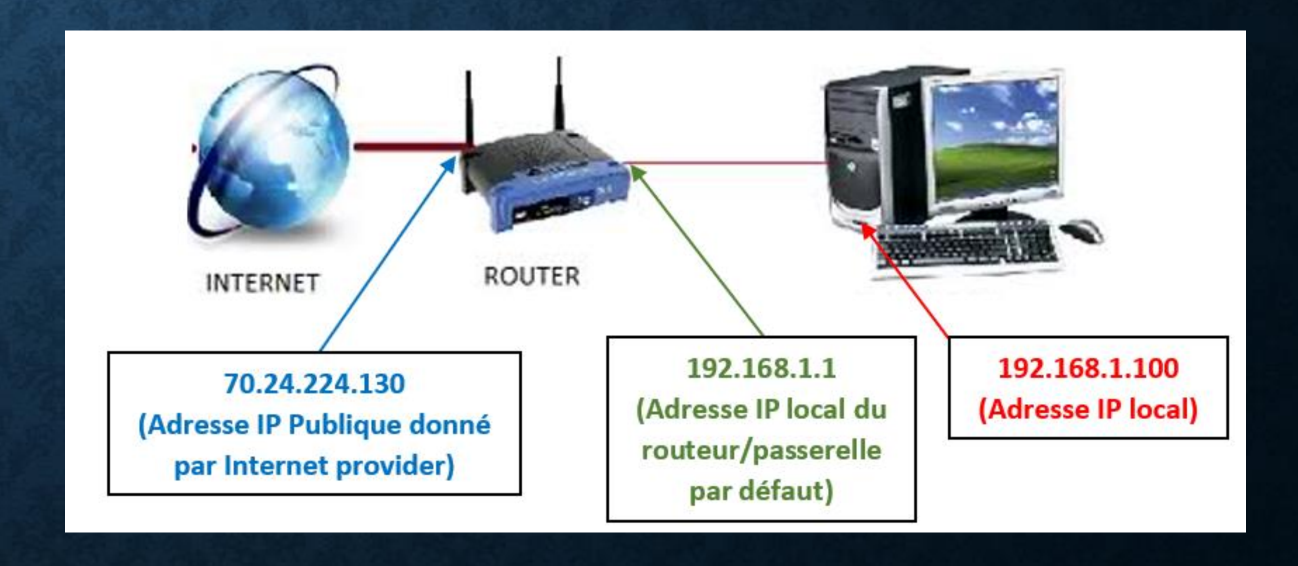
- Une technique d'attaque et de découverte consiste **à vérifier tous les ports ouverts d'une machine** pour énumérer les applications et services en cours de fonctionnement.

- On appelle cela le **scan de ports** ou **balayage de ports**.

LES PORTS RÉSEAUX - SCAN DEPUIS INTERNET

- Il existe des services en ligne qui permettent de scanner les ports ouverts. Example: https://hidemy.name/en/port-scanner/
- C'est **les ports ouverts de votre routeur** qui seront scanner depuis internet et non votre ordinateur, qui n'est pas directement accessible puisqu'il est placé derrière votre routeur.
- La plupart du temps, les ports vont être affichés comme **filtré** car le pare-feu de votre routeur est activé.





2- PARE-FEU - DÉFINITION

- Un firewall ou pare-feu est un logiciel ou équipement réseau placé entre deux réseaux pour filtrer les connexions entrantes et sortantes.

- Le pare-feu autorise ou refuse les connexions légitimes des connexions non légitimes.

- Ces autorisations d'accès peuvent se faire à partir **de règles établies par l'administrateur** ou de manière automatique selon par exemple le contenu des paquets réseaux qui transitent.

- Avec un firewall, vous pouvez potentiellement bloquer le trafic malveillant provenant d'une attaque ou le trafic sortant provenant d'un malware.

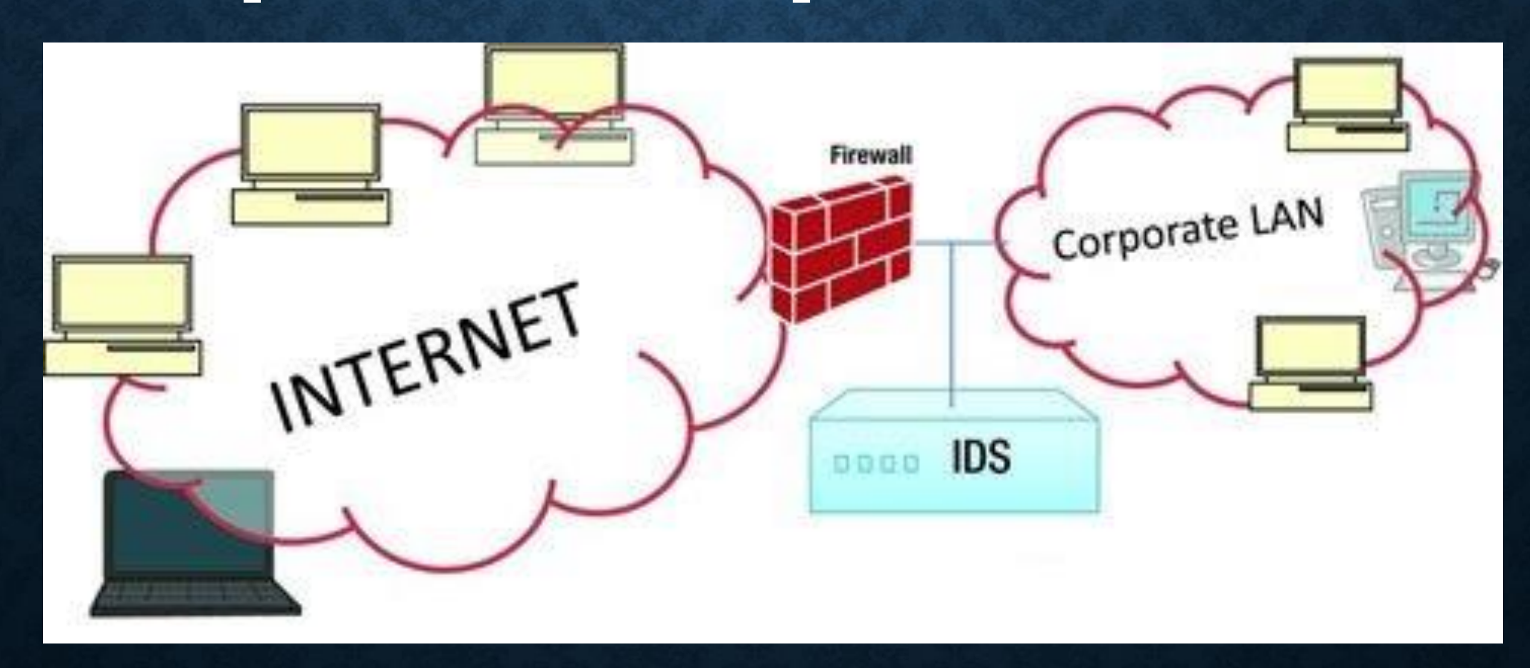


PARE-FEU - GÉNÉRATIONS

- Les premières générations filtre le contenu que sur les ports de connexion.
- Ainsi, si vous possédez un site WEB qui tourne sur le port 80 (HTTP), vous devez autoriser les accès sur ce port.
- Toutefois si un malware écoute sur ce port, la connexion sera autorisée.
- Les générations actuelles de pare-feu peut comprendre et lire les protocoles applicatifs.
- Ainsi, un pare-feu sait si un paquet concerne une application FTP ou HTTP, en créant les règles appropriées.

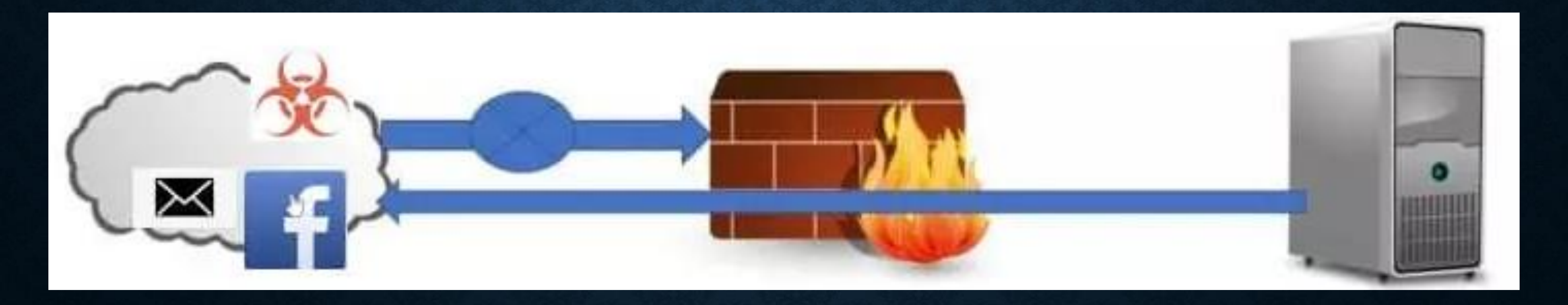
PARE-FEU - GÉNÉRATIONS

- Enfin les boitiers firewall embarquent des antivirus, ainsi que des IDS (Intrusion Detection System pour système de détection d'intrusion) capable d'analyser les paquets.
- Des signatures peuvent être intégrées afin de bloquer des paquets selon leurs contenues afin de bloquer certaines attaques.



3- LE FONCTIONNEMENT DU PARE-FEU

- Le pare-feu fonctionne sur **des règles** qui seront appliquées sur les paquets entrantes ou sortantes d'une interface réseaux contrôlées par le pare-feu.
- Celle-ci comporte généralement les données suivantes :
  - Une source (adresse IP ou Hôte) et un port TCP source.
  - Une destination (adresse IP ou Hôte) et un port TCP destination.
  - Parfois on trouve le statut de la connexion (nouvelle, établie).



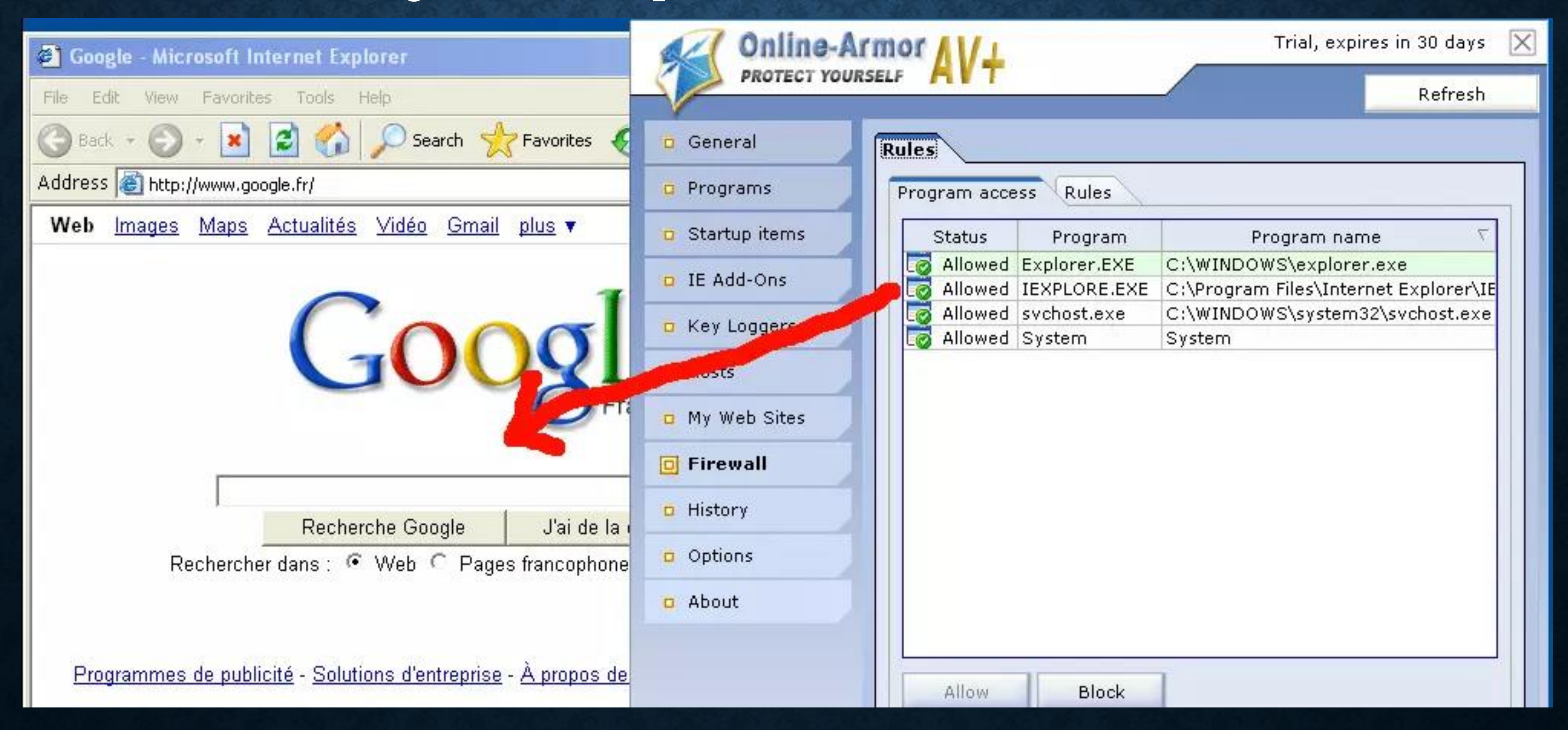
LE FONCTIONNEMENT DU PARE-FEU

- Par exemple, vous pouvez autoriser des connexion provenant de certaines adresses IP en source vers un port particulier puis faire une règle qui interdit toutes les connexions sur ce port.

6	Autoriser	TCP	192.88.134.0/23	443	Activé	
7	Autoriser	TCP	185.93.228.0/22	443	Activé	
8	Autoriser	TCP	66.248.200.0/22	443	Activé	
9	Refuser	TCP	tous	443	Activé	
10	Refuser	TCP	tous	80	Activé	

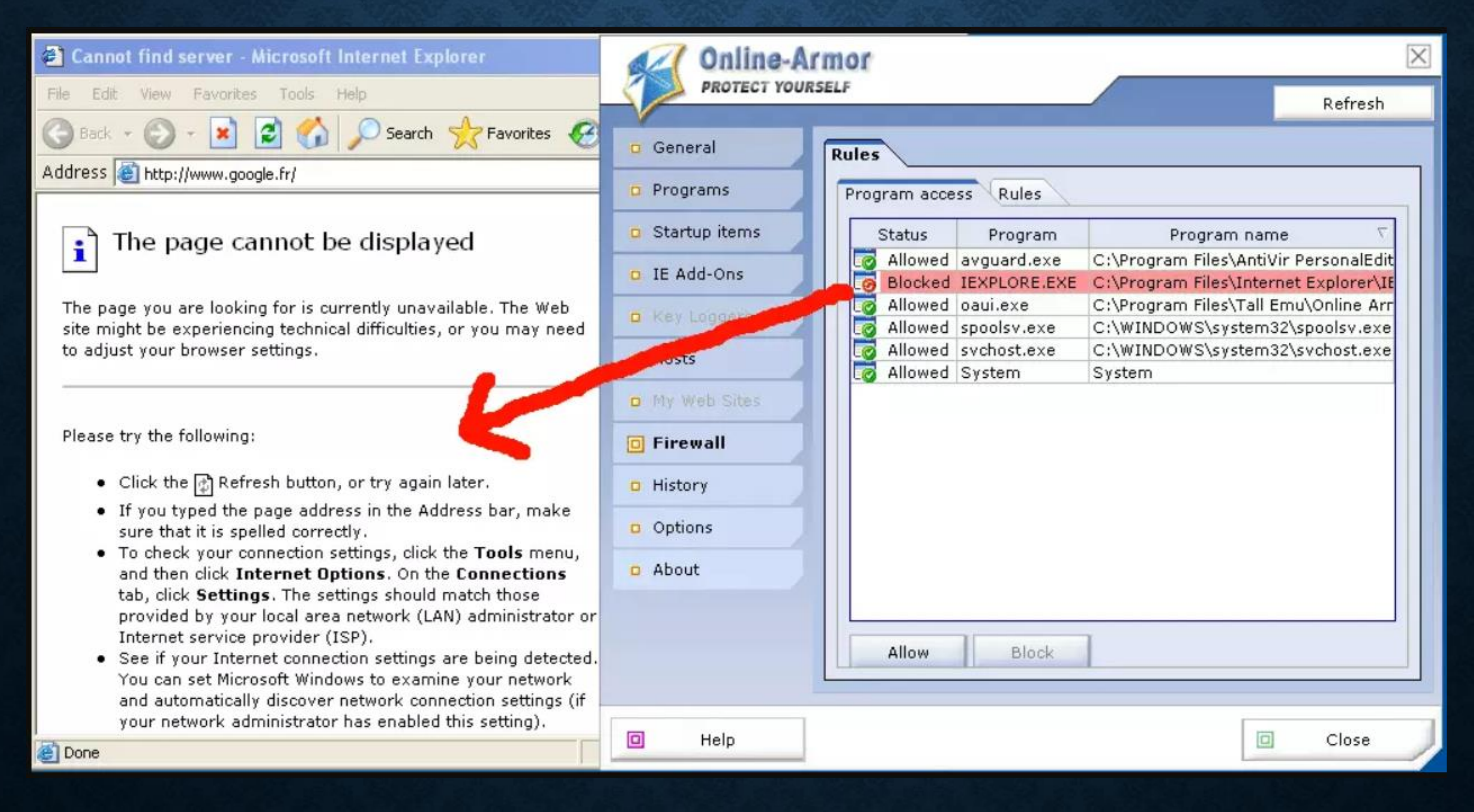
LE FONCTIONNEMENT DU PARE-FEU

- Le pare-feu fonctionne aussi sur des règles qui autorisent ou interdisent à telles ou telles applications de se connecte.
- Par exemple, ci-dessous, on constate à droite que le pare-feu autorise le processus iexplore.exe. La connexion vers le site Google est alors possible.



LE FONCTIONNEMENT DU PARE-FEU

- On passe alors Internet Explorer en rouge, interdiction… La connexion sur Google renvoi une erreur.



LE FONCTIONNEMENT DU PARE-FEU

- Lorsqu'un programme voudra établir une connexion entrante ou sortante, le pare-feu stoppera immédiatement la connexion et **vous demandera l'action à effectuer.**
- Vous avez généralement le choix entre :
  - Autoriser une fois la connexion ;
  - Autoriser tout le temps la connexion ;
  - Bloquer une fois la connexion ;
  - Bloquer tout le temps la connexion.
- Comprenez donc que ces règles sont très importantes, si vous autorisez un logiciel malveillant, ce dernier pourra se connecter et la connexion vers le centre de contrôle sera effective.
- Un pare-feu bloque automatiquement toute connexion non autorisée.

LE FONCTIONNEMENT DU PARE-FEU

- Les pare-feu sont donc extrêmement utiles pour prévenir l’installation de logiciels malveillants ou bloquer le fonctionnement des virus.
- Le Firewall peut entrer en jeu lorsqu’un Trojan Downloader, c’est à dire un trojan (le cheval de troie) qui tente de télécharger du contenu malveillant depuis internet.
- En bloquant le Trojan Downloader, ce dernier ne pourra pas télécharger le trojan et l’installer sur l’ordinateur.

- Le pare-feu peut aussi être utile pour bloquer la communication entre le cheval de troie et le serveur de contrôle du Hacker.
- Si le trojan ne peut se connecter il ne pourra pas échanger d’informations et ainsi livrer les données volées.

4- AUTRES FONCTIONNALITÉS

- Les fonctionnalités du pare-feu sont généralement différents selon le type de pare-feu (matériel, logiciel pare-feu Windows, etc).
- On trouve aussi une tableau de bord avec des statistiques de connexions et les journaux qui permettent de connaître les connexions bloquées ou autorisées par le firewall.

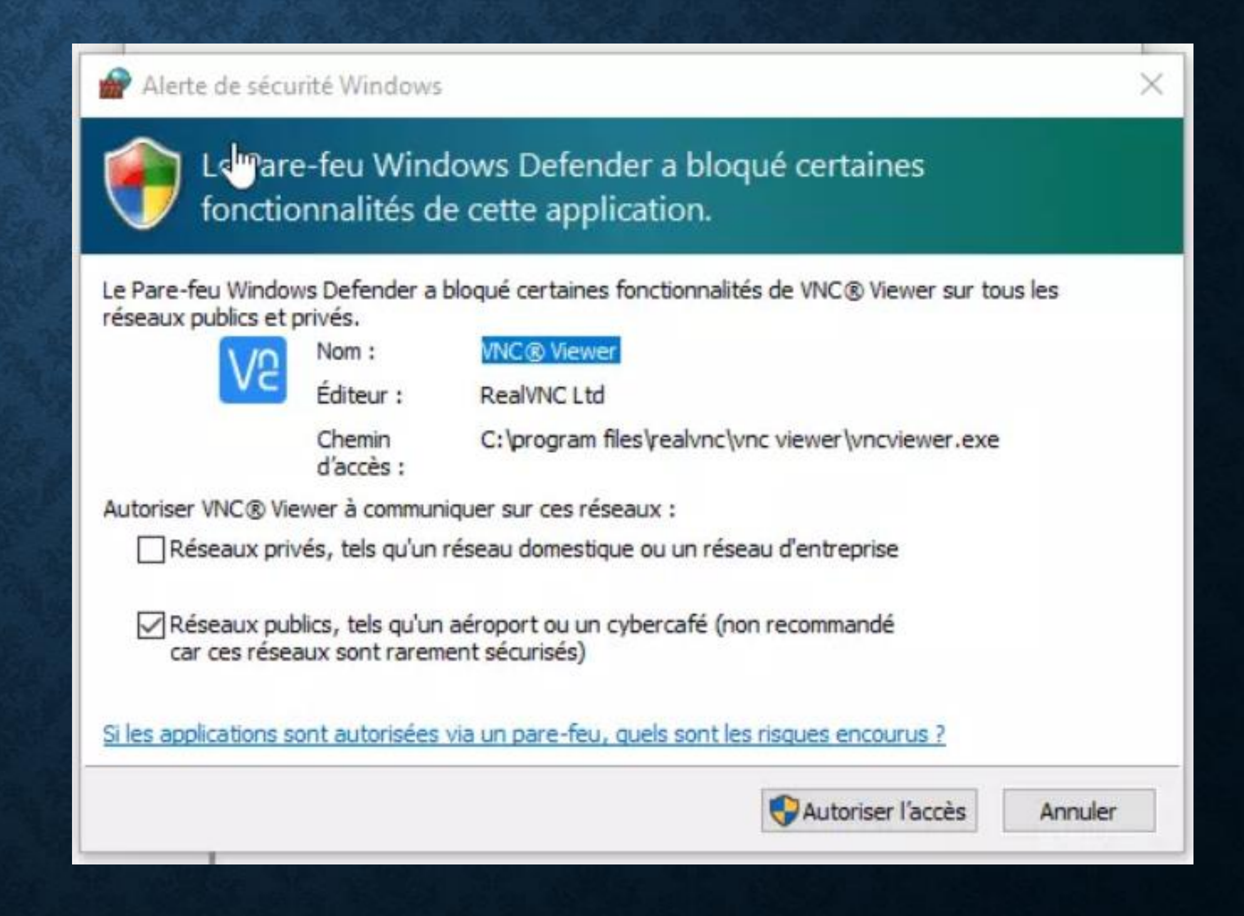
5- EXEMPLES DE PARE-FEU – WINDOWS DEFENDER

- Windows 10 intègre un pare-feu, **Windows Defender,** qui est capable de filtrer les connexions entrantes et sortantes pour les applications en cours d'exécution.

- On peut aussi établir ses propres règles selon les protocoles, ports ou adresses IP.

- Lorsqu'une nouvelle application tente d'émettre une connexion, une alerte de sécurité s'affiche et l'utilisateur doit autoriser ou non.

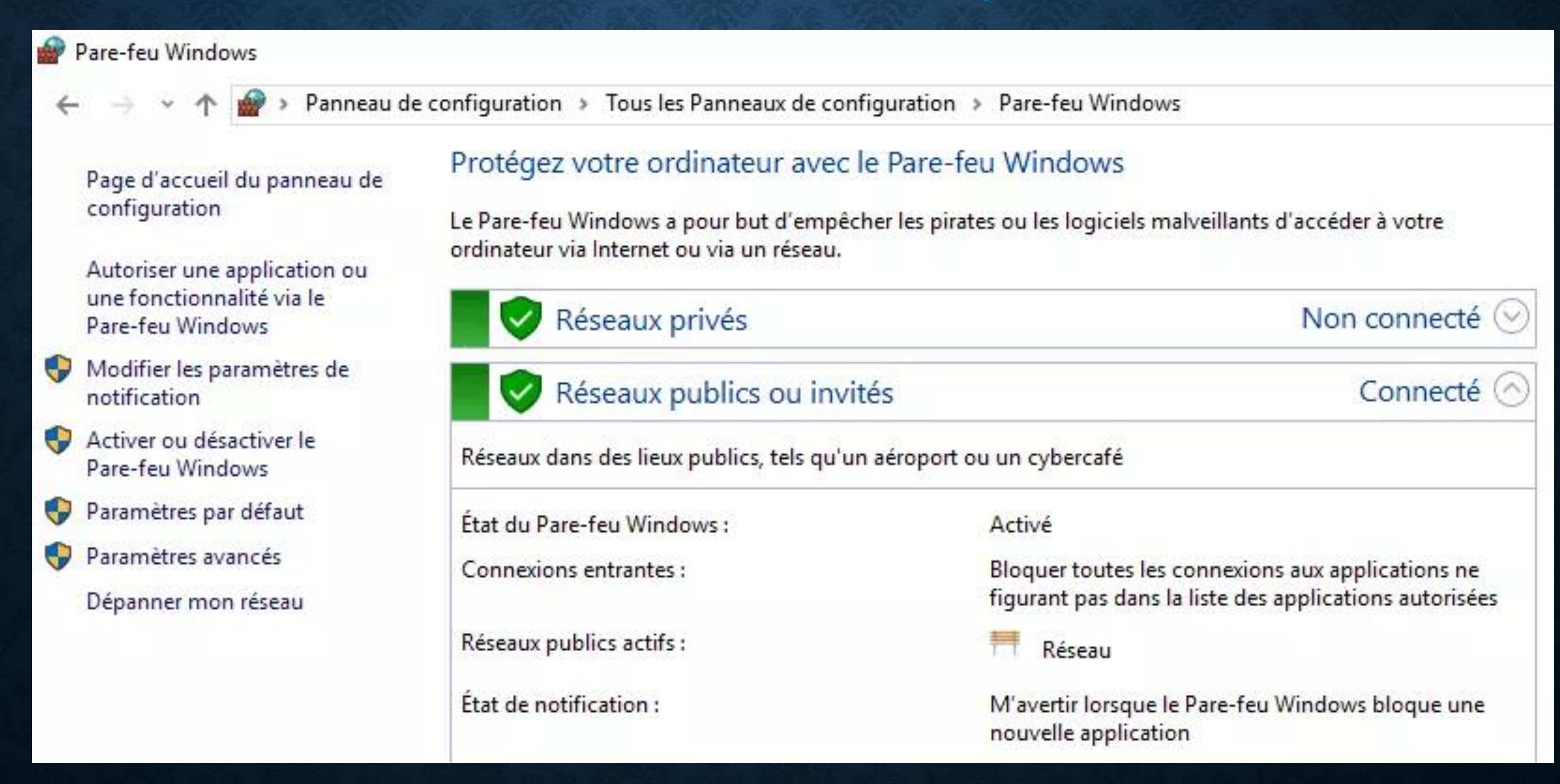
- À partir de là, une règle se créée afin d'autoriser ou non de manière permanente.



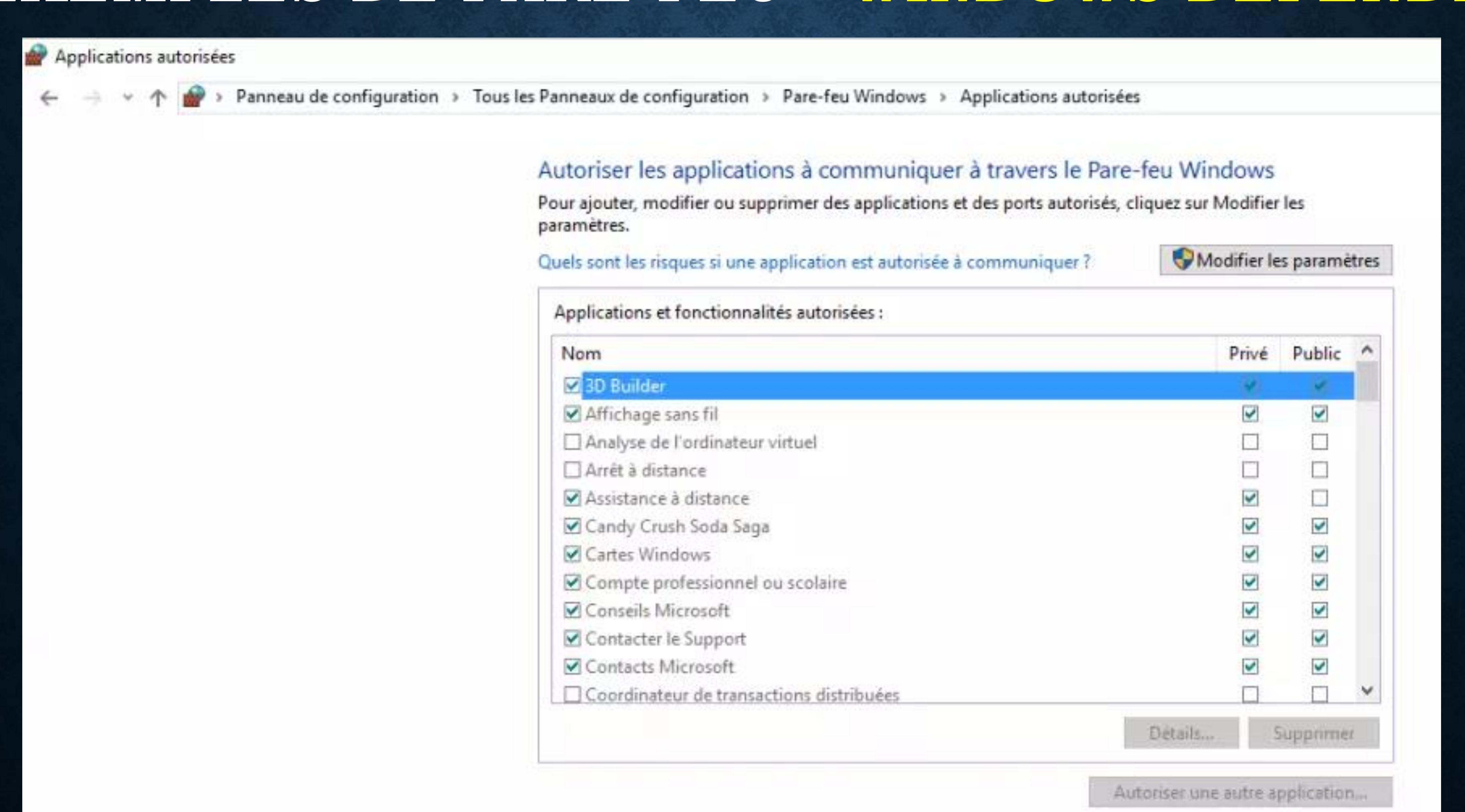
EXEMPLES DE PARE-FEU - WINDOWS DEFENDER

Le pare-feu de Windows se présente sous deux formes :

1. Une forme simplifiée avec des règles par applications ou ports.
   Les paramètres sont accessibles depuis le Panneau de configuration de Windows > Pare-feu Windows.

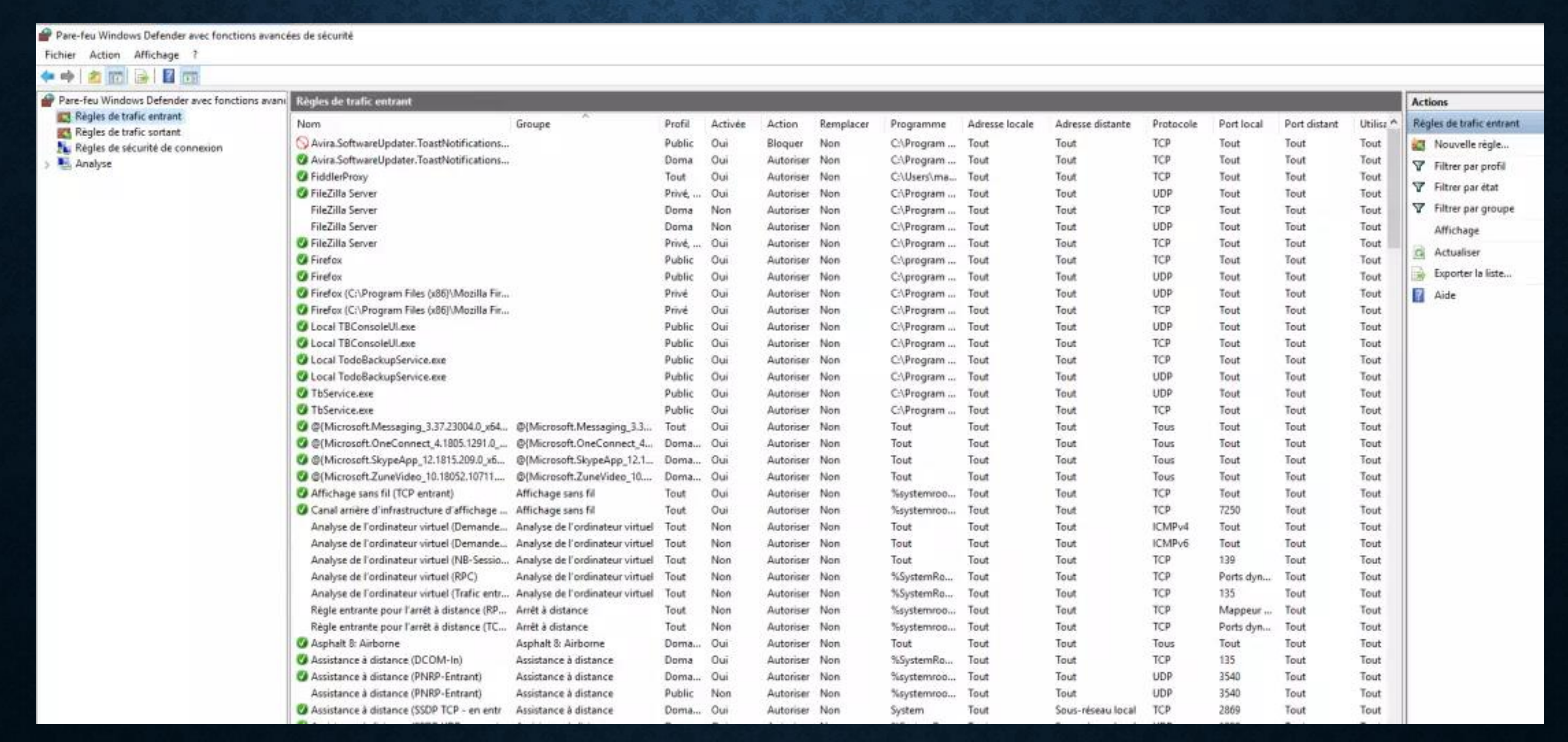


EXEMPLES DE PARE-FEU - WINDOWS DEFENDER



EXEMPLES DE PARE-FEU - WINDOWS DEFENDER

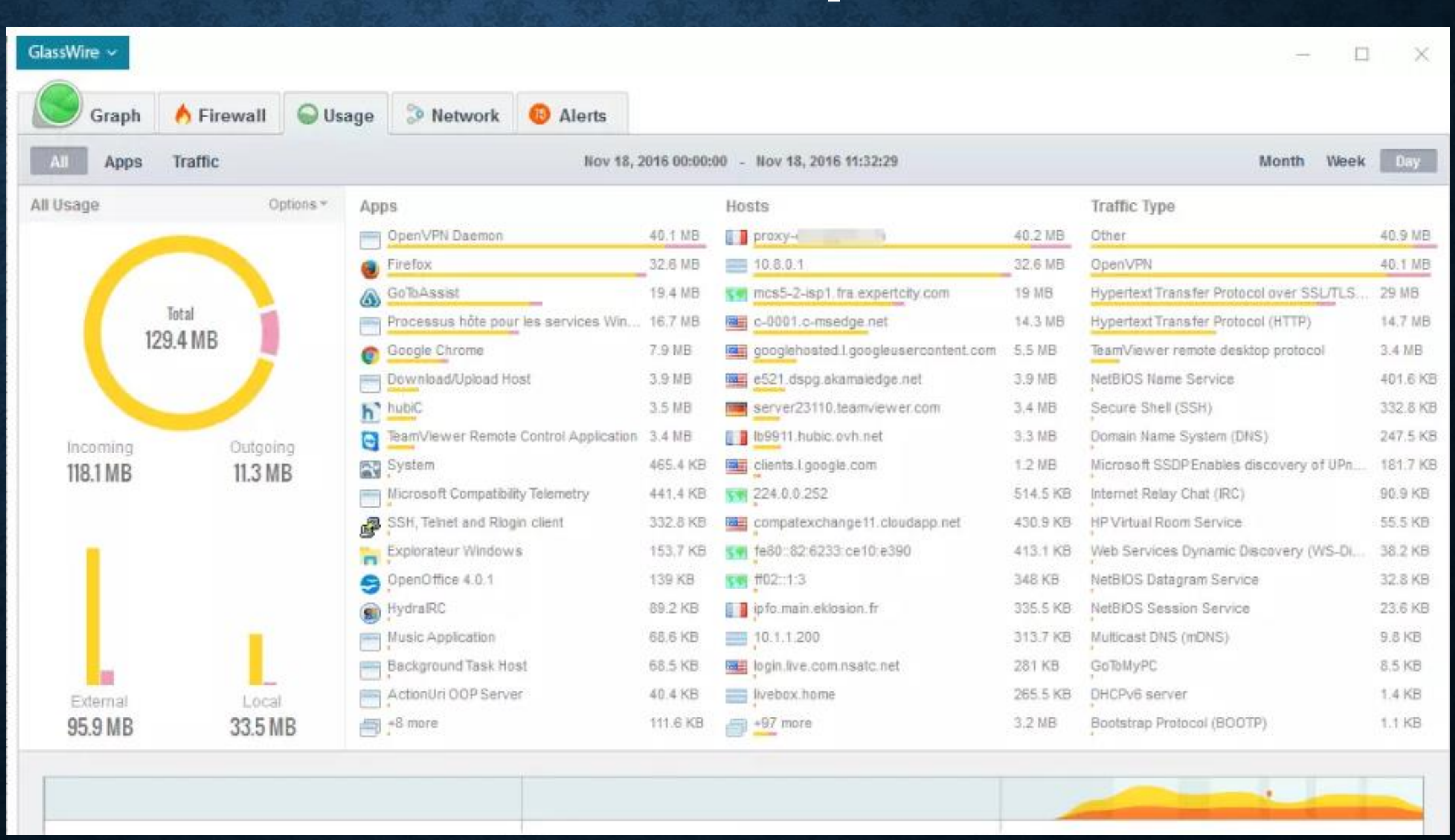
2. Une interface plus complexe et avancée où vous pouvez ajouter des règles.



Nom	Groupe	Profil	Activée	Action	Remplacer	Programme	Adresse locale	Adresse distante	Protocole	Port local	Port distant	Utilisa
Avira.SoftwareUpdater.ToastNotifications...		Public	Oui	Bloquer	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
Avira.SoftwareUpdater.ToastNotifications...		Doma	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
FiddlerProxy		Tout	Oui	Autoriser	Non	C:\Users\ma...	Tout	Tout	TCP	Tout	Tout	Tout
FileZilla Server		Privé, ...	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout
FileZilla Server		Doma	Non	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
FileZilla Server		Doma	Non	Autoriser	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout
FileZilla Server		Privé, ...	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
Firefox		Public	Oui	Autoriser	Non	C:\program ...	Tout	Tout	TCP	Tout	Tout	Tout
Firefox		Public	Oui	Autoriser	Non	C:\program ...	Tout	Tout	UDP	Tout	Tout	Tout
Firefox (C:\Program Files (x86)\Mozilla Fir...		Privé	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout
Firefox (C:\Program Files (x86)\Mozilla Fir...		Privé	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
Local TBConsoleUI.exe		Public	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout
Local TBConsoleUI.exe		Public	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
Local TodoBackupService.exe		Public	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
Local TodoBackupService.exe		Public	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout
TbService.exe		Public	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout
TbService.exe		Public	Oui	Autoriser	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout
@{Microsoft.Messaging_3.37.23004.0_x64...	@{Microsoft.Messaging_3.3...	Tout	Oui	Autoriser	Non	Tout	Tout	Tout	Tous	Tout	Tout	Tout
@{Microsoft.OneConnect_4.1805.1291.0_...	@{Microsoft.OneConnect_4...	Doma...	Oui	Autoriser	Non	Tout	Tout	Tout	Tous	Tout	Tout	Tout
@{Microsoft.SkypeApp_12.1815.209.0_x6...	@{Microsoft.SkypeApp_12.1...	Doma...	Oui	Autoriser	Non	Tout	Tout	Tout	Tous	Tout	Tout	Tout
@{Microsoft.ZuneVideo_10.18052.10711....	@{Microsoft.ZuneVideo_10....	Doma...	Oui	Autoriser	Non	Tout	Tout	Tout	Tous	Tout	Tout	Tout
Affichage sans fil (TCP entrant)	Affichage sans fil	Tout	Oui	Autoriser	Non	%systemroo...	Tout	Tout	TCP	Tout	Tout	Tout
Canal arrière d'infrastructure d'affichage ...	Affichage sans fil	Tout	Oui	Autoriser	Non	%systemroo...	Tout	Tout	TCP	7250	Tout	Tout
Analyse de l'ordinateur virtuel (Demande...	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	Non	Tout	Tout	Tout	ICMPv4	Tout	Tout	Tout
Analyse de l'ordinateur virtuel (Demande...	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	Non	Tout	Tout	Tout	ICMPv6	Tout	Tout	Tout
Analyse de l'ordinateur virtuel (NB-Sessio...	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	Non	Tout	Tout	Tout	TCP	139	Tout	Tout
Analyse de l'ordinateur virtuel (RPC)	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	Non	%SystemRo...	Tout	Tout	TCP	Ports dyn...	Tout	Tout
Analyse de l'ordinateur virtuel (Trafic entr...	Analyse de l'ordinateur virtuel	Tout	Non	Autoriser	Non	%SystemRo...	Tout	Tout	TCP	135	Tout	Tout
Règle entrante pour l'arrêt à distance (RP...	Arrêt à distance	Tout	Non	Autoriser	Non	%systemroo...	Tout	Tout	TCP	Mappeur ...	Tout	Tout
Règle entrante pour l'arrêt à distance (TC...	Arrêt à distance	Tout	Non	Autoriser	Non	%systemroo...	Tout	Tout	TCP	Ports dyn...	Tout	Tout
Asphalt 8: Airborne	Asphalt 8: Airborne	Doma...	Oui	Autoriser	Non	Tout	Tout	Tout	Tous	Tout	Tout	Tout
Assistance à distance (DCOM-In)	Assistance à distance	Doma	Oui	Autoriser	Non	%SystemRo...	Tout	Tout	TCP	135	Tout	Tout
Assistance à distance (PNRP-Entrant)	Assistance à distance	Doma...	Oui	Autoriser	Non	%systemroo...	Tout	Tout	UDP	3540	Tout	Tout
Assistance à distance (PNRP-Entrant)	Assistance à distance	Public	Non	Autoriser	Non	%systemroo...	Tout	Tout	UDP	3540	Tout	Tout
Assistance à distance (SSDP TCP - en entr	Assistance à distance	Doma...	Oui	Autoriser	Non	System	Tout	Sous-réseau local	TCP	2869	Tout	Tout

5. EXEMPLES DE PARE-FEU - PARE-FEU TIERS

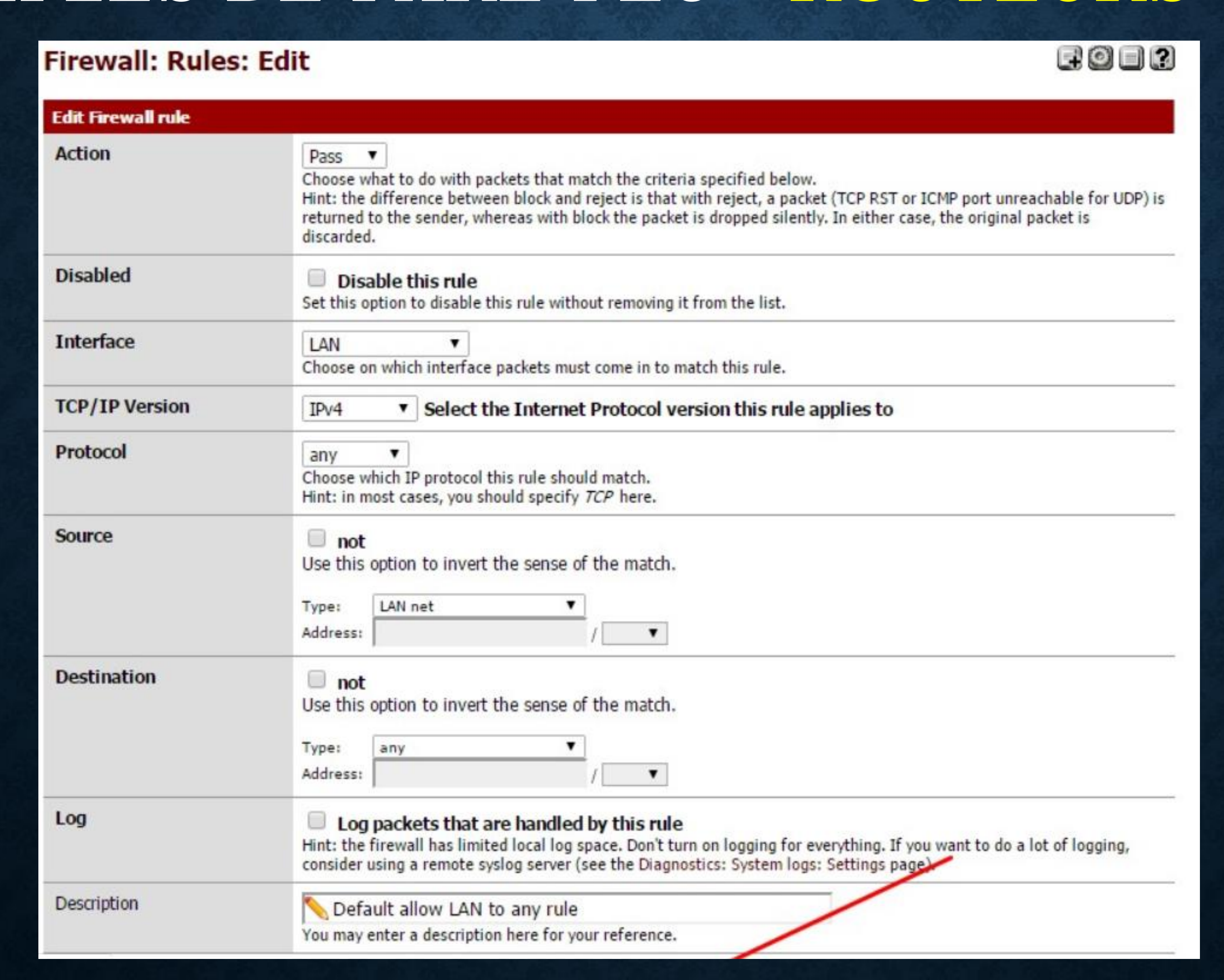
- Il existe aussi autres pare-feu pour Windows.
- Globalement le fonctionnement de ces derniers s'avèrent identiques.
- Example:
  - Glasswire
  - ZoneAlarm
  - Comodo Firewall



5. EXEMPLES DE PARE-FEU - ROUTEURS

- Le routeur à la maison agit partiellement comme pare-feu pour les ordinateurs du réseau local qui y sont connectés.
- Le routeur n'autorise que les connexions initialisées depuis le réseau local.
- C'est à dire qu'il va autoriser les connexions sortantes depuis un ordinateur du réseau local vers internet et bloquer les connexions depuis internet via ces ordinateurs (sauf si un transfert de ports a été configuré).
- Cependant, les connexions sortantes étant autorisées, toute connexion provenant de votre ordinateur vers un site est autorisé, donc potentiellement le téléchargement d'un Trojan par exemple, sauf si vous installez un pare-feu sur chaque ordinateur.

EXEMPLES DE PARE-FEU - ROUTEURS



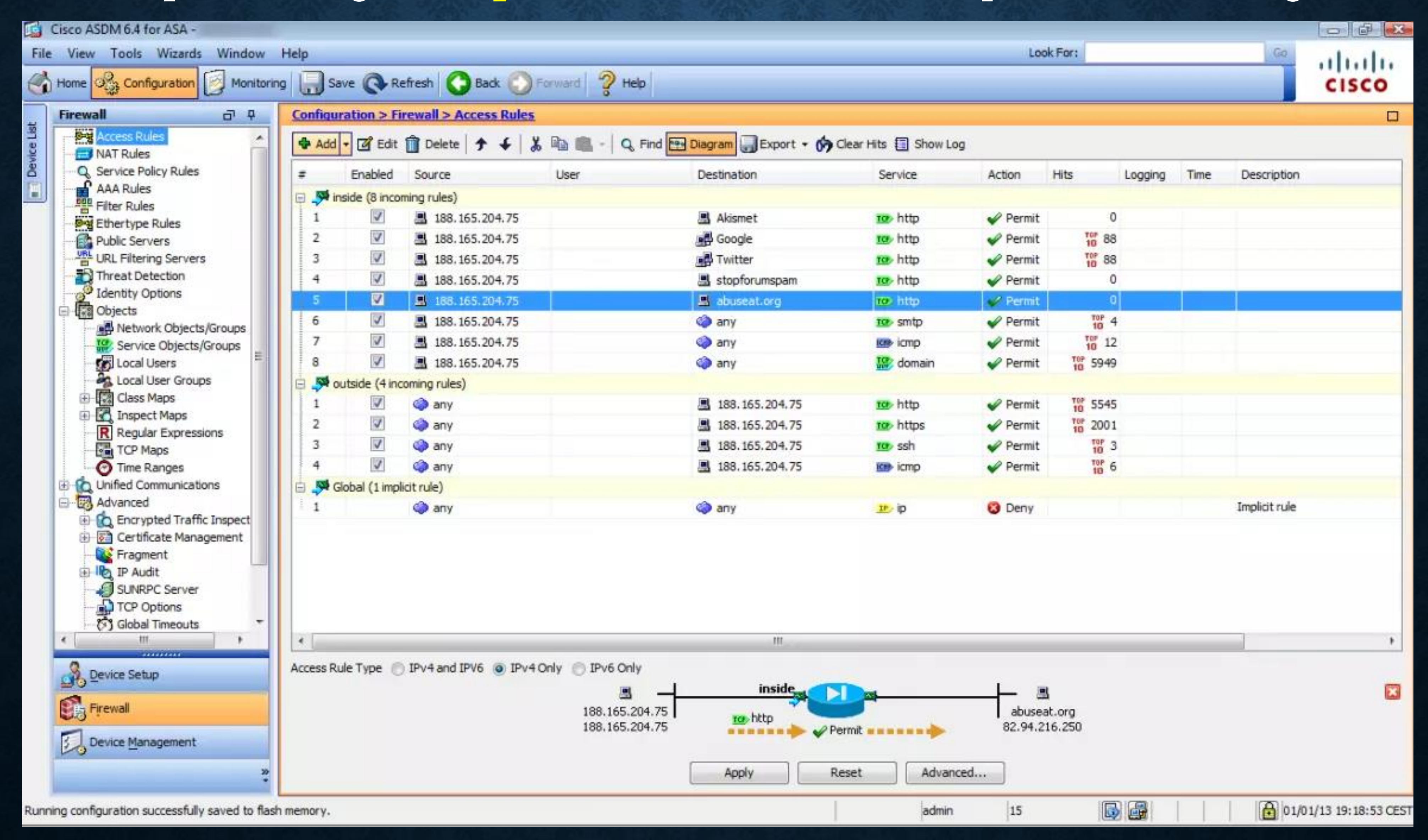
5. EXEMPLES DE PARE-FEU - BOITIERS FIREWALL

- Le Cisco ASA est un exemple des **boitiers Firewall** qui existent sous différents modèles et utilisé dans les entreprises.
- Example, le pare-feu Cisco ASA, série 5500-X est un pare-feu de nouvelle génération conçu pour vous aider à trouver le juste équilibre entre efficacité et productivité.
- Cette solution combine le pare-feu dynamique le plus déployé de l'industrie à un éventail complet de services de sécurité réseau de nouvelle génération, y compris :
  - Robuste sécurité Web, sur site ou en nuage;
  - Système prévention pour protéger les réseaux contre les menaces connues;
  - Protection complète contre les menaces et les programmes malveillants;
  - Pare-feu ASA le plus déployé au monde avec l'accès distant sécurisé.



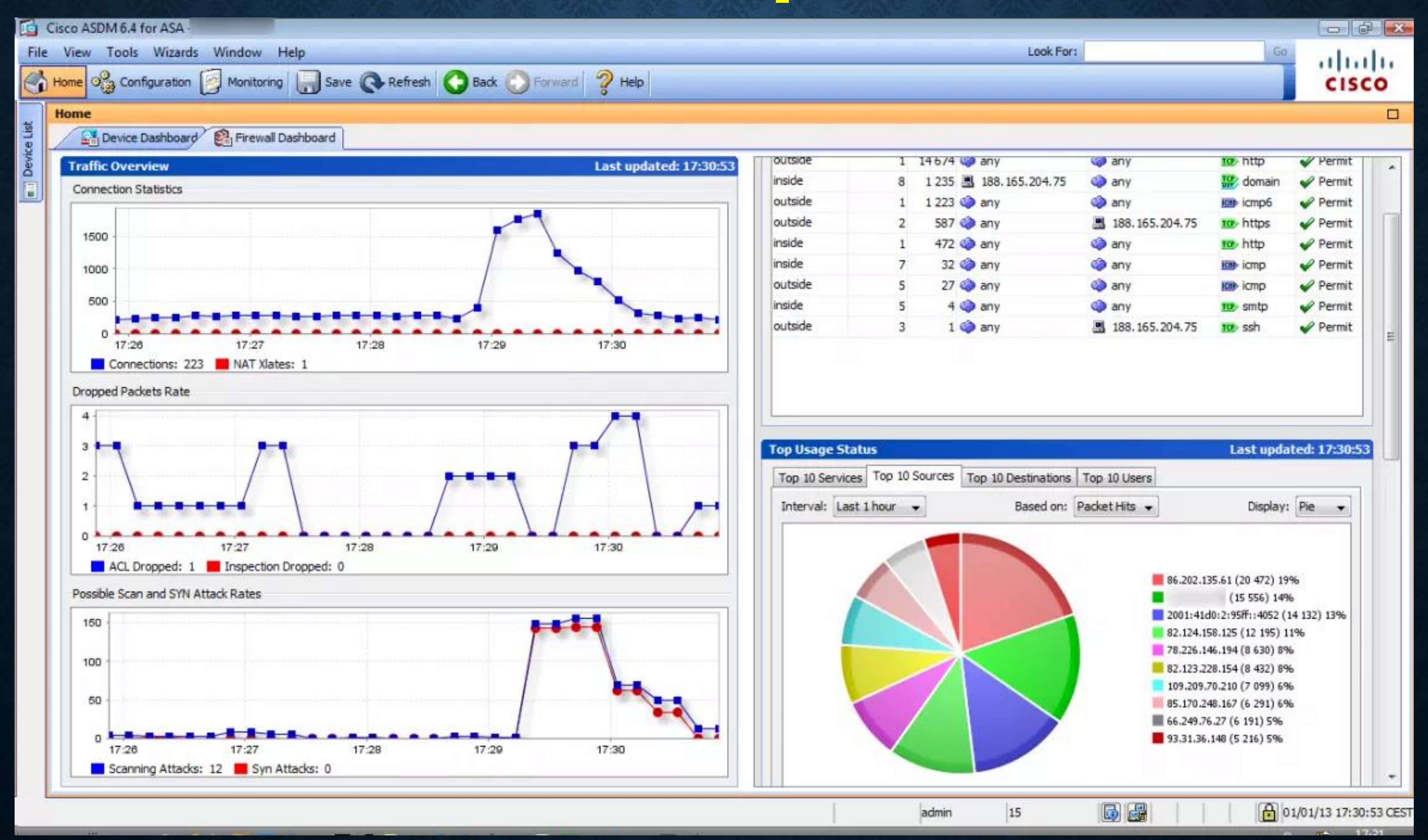
EXEMPLES DE PARE-FEU - **BOITIERS FIREWALL**

- Voici une exemple des règles de **pare-feu Cisco ASA** ainsi que toute la configuration.



EXEMPLES DE PARE-FEU - BOITIERS FIREWALL

- L'interface du **tableau de bord avec des statistiques** de connexion.



EXEMPLES DE PARE-FEU - **BOITIERS FIREWALL**

- Enfin **les journaux du pare-feu** avec les paquets dropés en temps réel.

